

**COLLEGE OF HEALTH & SCIENCE  
SCHOOL OF COMPUTING & MATHEMATICS**

**UNIT OUTLINE**

**300447 Computer Forensics Workshop  
(level 3, 10 credit points)  
Spring 2006**

**Location:** School of Computing and Mathematics  
Penrith Campus, Locked bag 1797, Penrith South DC NSW 1797  
General enquiries: 4736 0620

**Unit Coordinator:  
(and Lecturer)** **Derek Bem**  
Room Y326, Building Y, Penrith Campus, Email: [d.bem@uws.edu.au](mailto:d.bem@uws.edu.au)  
**Web:** <http://www.scm.uws.edu.au/compsci/computerforensics/>

**Lecturers:**

**Dr Yun Bai**  
Room Y360, Building Y, Penrith Campus, Email: [y.bai@uws.edu.au](mailto:y.bai@uws.edu.au)

**Dr Hon Cheung**  
Room Y327, Building Y, Penrith Campus, Email: [h.cheung@uws.edu.au](mailto:h.cheung@uws.edu.au)

**Dr Ewa Huebner**  
Room Y351, Building Y, Penrith Campus, Email: [e.huebner@uws.edu.au](mailto:e.huebner@uws.edu.au)

**Craig Linn**  
Room Y216, Building Y, Penrith Campus, Email: [c.linn@uws.edu.au](mailto:c.linn@uws.edu.au)

**Consultation:** The consulting times for the Unit Coordinator and the Lecturers are available on the web site below. All e-mails from enrolled students related to this unit will be answered within 2 working days.

**Unit web site:** <http://www.scm.uws.edu.au/units/2006.2/cfw/>

Students should be familiar with all University and College/School rules, policies and processes, related to their studies and time at UWS. Students should also be aware that they are required to abide by the University's Codes, Occupational Health and Safety and Social Justice policies.

Information on University, student rules, policies, procedures and codes can be found in the UWS Student Handbook, and online at on the Student Administration web page and the UWS Policy and Procedures web page.

Students should regularly check the Student Administration web page for updates, enrolment, timetabling and other related information. The above information can be found online at:

<http://www.uws.edu.au/students/stuadmin> and  
<http://apps.uws.edu.au/uws/policies/ppm/policies.phtml>

Students with a disability are advised to discuss requirements for accommodation (including for examinations) at the commencement of the teaching session with their Unit Coordinator in conjunction with the Counselling & Disabilities Unit within the Office of the Dean of Students. This is a free and confidential service, contact no: 02 4620 3018 or refer: [http://www.uws.edu.au/students/counselling\\_disability](http://www.uws.edu.au/students/counselling_disability)

UWS has a web page for students which contains links to the library, student support, including the free services offered by Office of the Dean of Students and other relevant information refer URL:  
<http://www.uws.edu.au/students>

## **Prerequisites**

300149 Operating Systems and  
300165 Systems Administration Programming and  
300143 Network Security  
**or approved equivalents.**

Students are advised that they are responsible for ensuring they have met all relevant pre-requisites and/or co-requisites for any unit(s) in which they are currently enrolled.

## **Non Award Students**

This unit is also offered for non award study to practicing computer professionals. In such case formal pre requisites do not apply, and each application is assessed on its merits by the unit coordinator.

## **Assumed Knowledge**

This unit requires a knowledge base of at least the level of a completed second year in a professional Computer Science degree, specifically operating systems internals, file systems, data representation, information security and the operation of a computer system. It is assumed that students are competent in using operating system interfaces and utilities, file systems, network facilities etc.

## **Teaching Schedule**

Lecture and laboratory sessions

All students should enrol in the lecture and one laboratory session of their choice. Please check [http://platformweb.uws.edu.au/pweb\\_tt/start.asp?yr=2006](http://platformweb.uws.edu.au/pweb_tt/start.asp?yr=2006) for the list of available laboratory sessions. The laboratory classes start in week 3.

Topics for lectures and laboratories are available on: Web site URL T.B.A.

## **Mode of Delivery**

- 2 hours of lecture per week for 13 weeks
- 4 hours of supervised practical work per week for 10 weeks

It is expected that students will spend additional 6 hours per week studying the subject material, preparing for the laboratory, and completing the required laboratory tasks.

## **Attendance Requirements**

Attendance at lectures is not compulsory, but students should note that lecture material may not be readily found in the recommended textbook, reference books and other printed materials. Attendance at laboratory classes is compulsory. Students should note that marks for practical work can only be obtained by demonstrating it to the tutor during the scheduled lab session. The tutor will not mark the work, which is submitted outside the lab time, electronically or in any other way. The lab reports should be submitted in hard copy to the tutor or to the lecturer one week after the scheduled lab session.

Students who missed the laboratory deadlines through illness or any other documented misadventure should contact the Unit Coordinator as soon as it is practically possible to arrange for marking of the missed assessment tasks. Depending on the circumstances a penalty may apply no higher than 10% of the mark for each working day after the deadline.

## **Purpose**

This unit is composed of a series of investigative workshops that put into practice, in a Computer Forensics context, many of the technical skills developed in earlier pre-requisite units. The unit is intended to not only further develop these skills but to instil: best technical practice, sound understanding of technical investigative techniques, and documentation of the results of investigation. Workshop topic areas include: clean media copying techniques, search and identification of hidden data, building profiles of computer activities through probing and analysis of log files, and how to prepare a system and network to best support subsequent intrusion and activity detection.

## **Objectives**

On the completion of the unit, students who have mastered all of its aspects will be able to:

- prepare forensically clean storage media to accept image copies of suspect media;
- perform an image copy from multiple storage media types without altering the source media;
- locate and identify data/files that are hidden or obfuscated on the media;
- reconstruct, in part or totally, deleted data or files that remain on the media;
- apply cryptographic and steganographic techniques where appropriate and viable;

- extract data from log files maintained by the operating system, web and email servers, and network proxies and firewalls;
- extract data from caches maintained by both server and client machines;
- analyse and interpret extracted log and cache data;
- document and present the results obtained from the above activities;
- use standard "off the shelf" software packages and hand written code to undertake the above tasks;
- perform the above tasks in multiple operating systems environments.

## Content

- Media preparation and copying techniques;
- File system structures and file type identification techniques;
- Applied cryptography and steganography (introductory only);
- The location, structure, and interpretation of log and cache based data associated with operating systems, web and email systems, and the network;
- Documentation and presentation standards;
- Selected industry standard software tools.

## Text Books

It is very difficult to recommend a single book (see also References note below). There are many topics covered, and each lecturer will specify what he/she considers to be the best resources for topics covered. Also the course is based heavily on detailed lecture notes and electronic materials in printable format, which allows each student to collect and print his/her own set of materials. A good general book which can be purchased from UWS bookshop is:

Jones, K., Bejtlich, R., & Curtis, R. *Real Digital Forensics: Computer Security and Incident Response*, Penguin Books Pearson Publishing, 2005.

## References

**Note:** The list of references is continually updated, and most books should be available in the closed reserve in Allen Library, Kingswood Campus. Please see <http://www.cit.uws.edu.au/compsci/computerforensics/> for current list of good books. Any book can be also order from UWS bookshop. Some titles are listed below, but this is not a complete list, there are many more:

Britz, M.T. *Computer Forensics and Cyber Crime An Introduction*. Pearson Prentice Hall, Upper Saddle River, USA, 2004.

Carrier. *File System Forensics*, Penguin Books Pearson Publishing, 2005.

Carvey, H. *Windows Forensics and Incident Recovery*, Penguin Books Pearson Publishing, 2004.

Dan Farmer, D., Venema, W. *Forensic Discovery*, Addison Wesley Professional, January 2005

Jones, K., Bejtlich, R., & Curtis, R. *Real Digital Forensics: Computer Security and Incident Response*, Penguin Books Pearson Publishing, 2005.

Kruse, W.G., & Heiser, J.G. *Computer Forensics Incident Response Essentials*. Addison Wesley Press, Boston, USA., 2002

Vacca, J.R., *Computer Forensics: Computer Crime Scene Investigation*, Second Edition Charles River Media, Inc., Hingham, MA, USA, 2005

## Assessment

The unit's assessment is all continuous, there is no final exam. Assessment items are as follows, all are based on individual student work:

Workshop Reports	75%
Minor Assignment @ 10%	10%
Major Assignment @ 15%	15%

The final grades in this unit will be awarded as follows:

- Pass – final mark more or equal 50 and less than 65
- Credit – final mark more or equal 65 and less than 75
- Distinction – final mark more or equal 75 and less than 85
- High Distinction – final mark equal or more than 85

Students should note, that final marks and grades are subject to confirmation by the School and College Assessment Committees, who may scale, modify or otherwise amend the marks and grades for the units, as may be required by University Policies.

## Special Consideration

Students should notify the University when they have suffered misadventure, or have extenuating circumstances which means they have:

- been prevented from meeting an assessment deadline;
- performed below their usual standard during an assessment, including formal examinations;
- been unable to attend a compulsory component of their course;
- been unable to attend a formal (end-of-session) examination.

The University has specific criteria, requirements (eg supporting documentation) and set deadlines for applying for special consideration and students are strongly encouraged to read the relevant sections of the Assessment and Examinations Policy refer URL: <http://apps.uws.edu.au/uws/policies/ppm/policies.phtml> and in particular the sections relating to: Matters Affecting Assessment and Inability to Attend an Examination

## Academic Misconduct

The University takes any form of academic misconduct seriously. Academic misconduct is conduct on the part of a student, which involves amongst other forms of misconduct: Cheating, Plagiarism and Collusion

For the full definition of academic misconduct and the consequences of such behaviour, students are advised to read the Academic Misconduct policy in its entirety, refer URL: <http://apps.uws.edu.au/uws/policies/ppm/policies.phtml>

## Disclaimer:

The material in this unit outline is accurate at the time of writing. Since variations may be necessary as the session progresses, students must ensure that they are aware of any announcements made in lectures and tute/prac sessions. The web and e-mail will be used extensively as a means of broadcasting information to students as well, so it is suggested that students check the web and their electronic mailboxes at least twice a week. Any changes will not be allowed as grounds of appeal for examination review etc.

© University of Western Sydney, 2006